La Ciberseguridad en el Ejercicio de la Abogacía

Jiménez Cuestas, Oscar Javier
Universidad Piloto de Colombia
Bogotá D.C., Colombia
oskrjim@hotmail.com

Resumen—El uso de las nuevas tecnologías, la seguridad de la informacióny la protección de datos que circulan a diario a través de las redes y medios tecnológicos se han convertido en un tema de amplio debate en el mundo y han generado la creación de políticas y medidas de prevención y protección frente a los ciberataques.

En Colombia esta preocupación se ha centrado en entidades públicas y financieras. Sin embargo, la ciberseguridad debe ser un tema que preocupe a otros sectores sociales y económicos.

Los profesionales del derecho no pueden estar al margen y deben adaptarse al reto de la ciberseguridad. El deber de un abogado actual debe ir más allá de usar las diversas herramientas tecnológicas que facilitan su labor. Es también su deber la implementación de sistemas, normas o modelos que garanticen la seguridad de la información y la protección de la gran cantidad de datos sensibles presentes en los procesos judiciales que hacen parte de su quehacer diario.

El éxito de los procesos judiciales de hoy depende del uso adecuado de la tecnología, la administración de la información, la aplicación de los principios de confidencialidad, integridad y disponibilidad y la construcción de despachos de abogados ciberseguros.

Índice de Términos—Ciberseguridad, Colcert, Despacho de abogados, Protección de datos, Confidencialidad, integridad, disponibilidad.

Abstract—*The use of new technologies, the security of information and the protection of the data circulating through networks and technological means have become a subject of wide debate in the world and have generated the creation of policies and measures . The prevention and protection against cyber attacks.*

In Colombia, this concern has focused on public and financial entities. However, cybersecurity should be an issue that concerns other social and economic sectors.

Law professionals can not be on the sidelines and must adapt to the cybersecurity challenge. The duty of a current lawyer must go beyond using the various technological tools that facilitate their work. It is also your duty to implement systems, standards or models that guarantee the security of information and the protection of the large amount of sensitive data present in the judicial processes that are part of your daily work.

The success of today's judicial processes depends on the use of technology, the administration of information, the application of confidentiality principles, integrity and availability, and the construction of cybersecurity law firms.

Keywords—*Cybersecurity, Colcert, Law Firm, Data protection, Confidentiality, integrity, availability.*

I. INTRODUCCIÓN

En la actualidad la tecnología hace parte de nuestra vida cotidiana y el uso de las nuevas herramientas digitales pueden ser determinantes a la hora de ejercer cualquier profesión. El ejercicio de la abogacía es un rol indispensable en la sociedad que no ha podido estar al margen del constante desarrollo tecnológico.

Colombia ha tenido una serie de reformas legales que representan cambios sustanciales en los procedimiento judiciales. Hemos pasado de procesos arcaicos llenos de toneladas de papel, a hacer uso de la tecnología para facilitar el acceso a la justicia y la celeridad de los procesos. El reto de los abogados de hoy va más allá de obtener resultados positivos dentro de los procesos judiciales. Es su deber dar un uso adecuado y responsable a la tecnología, dando prioridad al desarrollo e implementación de la seguridad de la información y la protección de los datos que administran en el ejercicio de su labor.

La ciberseguridad en Colombia ha desarrollado mecanismos para prevenir o minimizar ataques, principalmente al interior de las entidades públicas y algunas entidades privadas, como las dedicadas a prestar servicios financieros. Pero el desarrollo debe amplificarse y preocupar a otros sectores de la sociedad, como es el caso de los bufetes o despachos de abogados que sin duda administran una gran cantidad de información sensible que debe protegerse.

"Los despachos de abogados, como instituciones y todos los responsables del derecho deben conocer el cambio de cultura jurídica y digital en el que nos encontramos y conocer el enfoque de la ciberseguridad como componente de la seguridad nacional".[1]

II. LA CIBERSEGURIDAD

La Ciberseguridad es un tema que preocupa al mundo entero y que se ha convertido en un amplio tema de debate dado el rápido desarrollo de las tecnologías y la vulnerabilidades de la información que constantemente circula a través de éstas.

La tecnología ha hecho posible la comunicación con personas que se encuentren en cualquier latitud, pero también ha permitido que los criminales logren infiltrarse y extraer información sensible y reservada, particularmente de las

entidades gubernamentales. Han sido objetivo de ciberataques el Congreso, la Casa Blanca y el Departamento de Seguridad Interna de Estados Unidos.

Entorno a esta preocupación se ha creado un abundante marco normativo nacional e internacional que se expone a continuación:

1) Internacional:

- Convenio sobre ciberdelincuencia del Consejo de Europa (2004)
- Resolución AG/RES 2004 de la Asamblea General de la Organización de Estados Americanos (OEA)
- Decisión 587 de la Comunidad Andina (2004)
- Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT (2005)
- Resolución 64/25 de la Asamblea General de las Naciones Unidas (2009)
- Directiva 2006/24 de la Unión Europea

2) Nacional

- ***Artículo 15 de la Constitución Política de Colombia***

"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

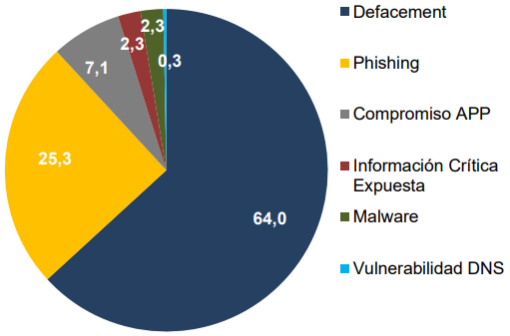
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley" [2]

- **Ley 527 de 1999,** relacionada con el Comercio electrónico.
- Ley 1266 de 2008, o Ley del Habeas Data
- Ley 1273 de 2009: Ciberdelitos
- Conpes 3701
- Conpes 3854
- Circular 007 de 2018 (Entidades Financieras)

III. LA CIBERSEGURIDAD EN COLOMBIA

Uno de los Ciberataques más significativos en la historia de Colombia data en 2011, cuando un grupo denominado Anonymous en señal de protesta frente a la Ley "Lleras" que pretendía penalizar la piratería informática, decidió atacar importantes páginas Gubernamentales como la del Ministerio de Interior y de Justicia, la del Senado de la República, Gobierno en Línea e incluso la página Web de la Presidencia de la República. Situaciones como ésta han propiciado la creación de políticas orientadas a minimizar los riesgos de amenazas o ataques cibernéticos.

Según información de Asobancaria el siguiente gráfico refleja el comportamiento según el tipo de ataques registrados en Colombia durante el 2017:



Fuente: Colcert. Elaboración Asbancaria

Fig 1. Asobancaria. Tipos de ataques registrados en Colombia[3]

El Estado a través del documento Conpes 3701 define ciberseguridad *"como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética."* [4].

Con la aprobación del Conpes 3701 de 2011 Colombia se convirtió en uno de los primeros países en Latinoamérica con propuestas orientadas a enfrentar delitos informáticos y minimizar los riesgos relacionados con amenazas de origen cibernético. Con éste se crearon grupos encargados de proteger a los cibernautas y los sistemas de información[5].

En septiembre de 2011 nace Colcert una entidad interinstitucional con la participación del Ministerio de Justicia, el Ministerio de Defensa y el Ministerio de TICs. COLCERT está vigilada por la comisión intersectorial quien es la encargada de establecer las políticas respecto a la gestión de la infraestructura tecnológica, información pública, ciberseguridad y ciberdefensa. ColCERT es creado con el objetivo de brindar un servicio de prevención ante amenazas informáticas, respuesta a incidentes y sensibilización en materia de seguridad informática.

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT será el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa. Prestará su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC." [6]

En 2016 se publicó el documento Conpes 3854, el cual incluye una nueva prioridad enfocados a la gestión de riesgos donde la política nacional de seguridad digital tendrá como objetivo fortalecer las capacidades de las partes interesadas, identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

El Estado Colombiano busca difundir, implementar, desarrollar, capacitarse, y fortalecer cada día los organismos como lo son COLCERT, SSIRT, OCCO, y el CCP, para así tener una mejor gestión estratégica para prevenir ataques cibernéticos.

1) Entidades Financieras

El sector financiero es un blanco seguro de los cibercriminales que buscan principalmente extraer información que permita acceder al dinero de sus víctimas. El experto del Cuerpo Técnico Investigativo (CTI) de la Fiscalía General de la Nación, Álvaro Colmenares, señaló que los delitos informáticos han tenido un gran crecimiento, pues, respecto de años anteriores, entre enero y febrero de 2017 se registró un incremento de denuncias de este tipo de delito del 26.34%, mientras que en el mismo periodo de 2018 esta cifra superó el 60%. Indicó además que el hurto a cuentas bancaria es una de las modalidades de hurto en aumento. [7]

La Superintendencia financiera, entidad encargada de la vigilancia de las entidades financieras en el país, define la ciberseguridad como "*el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger a los consumidores financieros y los activos de la entidad en el ciberespacio"* [8].

Según Asobancaria es el sector financiero uno de los que más invierte en la protección de datos y la incorporación de prácticas de ciberseguridad y seguridad de la información [9]

En el siguiente gráfico Asobancaria refleja el comportamiento de los ciberataques por sectores económicos, siendo el sector financiero el más atacado:

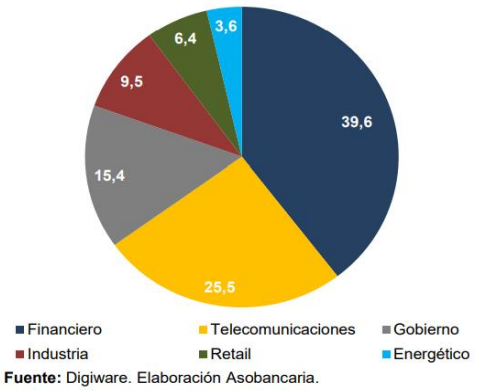


Fig 2. Asobancaria. Sectores más atacados. [10]

Los ataques cibernéticos y la importancia de la ciberseguridad es un tema que ha preocupado a diversos países del mundo desde hace más de dos décadas y frente al que se han tomado medidas significativas. En Colombia es un tema bastante nuevo, principalmente en entidades de tipo privado. Aunque el sector financiero ha sido uno de los sectores más afectados hasta apenas este año, la Superintendencia Financiera de Colombia expidió la Circular 007, mediante la cual se imparte instrucciones relacionadas con los requerimientos mínimos para la gestión de riesgos de ciberseguridad.

Mediante la Circular 007 de 2018, se estipulan las etapas que como mínimo deben considerar las entidades del sector financiero para la gestión de la seguridad de la información y la ciberseguridad, así:

- Prevención
- Protección y detección
- Respuesta y comunicación
- Recuperación y aprendizaje

IV. NORMA NTC-ISO-IEC-27001

"Norma técnica Colombiana NTC-ISO-IEC 27001, es una adopción idéntica por traducción de la norma ISO/IEC 27001:2013."

La norma suministra el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información, basándose principalmente en la protección de la confidencialidad, integridad y disponibilidad de ésta, a través de la aplicación de un proceso de gestión de riesgo.

Esta norma también incluye los requisitos para la valoración y tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización.

Dentro de la norma se encuentra el anexo A, donde se establece una lista de objetivos de control y controles que van desde el numeral 5 al 18 con un total de 114 controles; los cuales deben utilizarse para el tratamiento de riegos de la información. Es importante verificar que no se han omitidos controles necesarios dentro de la organización.

En los objetivos de control y controles del anexo A se describen tanto políticas como procedimientos que deberían implementarse en una organización, a continuación se mencionara las políticas que nos recomienda la norma NTC-ISO IEC 27001:

A.5.1.1	Políticas para la seguridad de la información
A.6.2.1	Política para dispositivos móviles
A.6.2.2	Política para Teletrabajo
A.9.1.1	Política de control de acceso
A.10.1.1	Política sobre uso de controles criptográficos

A.10.1.2	Gestión de llaves
A.11.2.9	Política de escritorio limpio y pantalla limpia
A.12.3.1	Respaldo de información
A.13.2.1	Políticas y procedimientos de transferencia de información
A.14.2.1	Política de desarrollo seguro
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores
A.18.1.4	Proteccion de informacion de datos personales

Tabla 1. Anexo A: Objetivos de control y controles. [11]

V. EL SECRETO PROFESIONAL DEL ABOGADO Y LA PROTECCIÓN DE DATOS.

Los procesos judiciales son un cúmulo de información y documentos con los que se pretende demostrar una situación jurídica.

Cédulas de ciudadanía, certificaciones bancarias, información confidencial de una organización, la intimidad de una familia y de una persona, son apenas algunos ejemplos de la información que puede estar presente en un proceso judicial.

La compañía europea *Abogado Compliance* [12],experta en asesorías de sistemas de gestión de protección de datos, describe cuáles son los posibles riesgos corporativos a los que pueden enfrentarse lo abogados en el ejercicio de su profesión así:

1. Suplantación de identidad: Creación de perfiles falsos para acceso a sistemas de información con uso de técnicas como phishing, pharming, registro ilícito de un nombre de dominio.
2. Ataques de denegación de servicios: colapso del sistema de información del despacho de abogados, infección de dirección IP.
3. Fugas de información: Robo de información con el uso de software malicioso, como datos personales de los clientes.

Cada documento que se incorpora a un proceso judicial tiene un valor probatorio indispensable y la protección de los mismos debe ser una de las principales preocupaciones de un abogado.

El artículo 28 de la Ley 1123 de 2007 (Código Disciplinario del Abogado), contempla los deberes profesionales del abogado. El numeral 9 del artículo en mención establece que es deber del abogado " *Guardar el secreto profesional, incluso después de cesar la prestación de sus servicios"*[13]. En España, a través del Real Decreto 658 de 2001 se describe el secreto profesional como un deber de los abogados así *"los abogados deberán guardar secreto de todos los hechos o noticias que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos".* En ambas legislaciones es claro que este deber va más allá de la duración de la prestación del servicio profesional. Así mismo, faltar a este deber se convierte en una falta disciplinaria para el abogado.

En países como España, el deber del secreto profesional va más allá de no revelar la información que sea de conocimiento del abogado en el ejercicio de su profesión. Según la autora Lourdes Sanz Calvo [14], el deber del secreto profesional consiste en *"Salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y en definitiva el poder de control o disposición sobre sus datos … se trata de impedir que los datos personales de cualquier titular puedan conocerse arbitraria e indiscriminadamente por terceros".*

En España las Leyes Orgánica 5 de 1992 y 15 de 1999 son las encargadas de regular el tratamiento y protección de los datos de carácter personal. En Colombia es la Ley 1266 de 2008 o Ley de Habeas Data la que contempla el derecho a la protección de datos personales. Sin embargo, en España del deber del secreto profesional ha ido más allá e integra el deber de protección de la información que hace parte de un proceso judicial y que debe ser protegida por el abogado.

VI. LA CIBERSEGURIDAD EN LOS DESPACHOS JUDICIALES

"Los ataques informáticos a despachos de abogados se han convertido en recurrentes en los últimos tiempos. Appleby, el cuarto despacho de actividades offshore más grande del mundo reconoció que en 2016 sufrió un robo de datos de sus clientes. El ataque a Mossack Fonseca, más conocido como los papeles de Panamá, dio lugar a la filtración de un enorme volumen de datos de sus clientes. DLA Piper, uno de los despachos más grandes del mundo, sufrió los efectos de los piratas informáticos con un ciberataque que destruyó 2.500 servidores e infectó 7.000 ordenadores. También la firma Senn Ferrero, fue objeto de otro famoso ataque que saltó a los medios como el caso Football Leaks" [15]

1) España:

España ha mostrado un gran interés entorno a la generación de políticas que permitan la protección de los datos y la información que hace parte de la labor de los abogados y sus despachos.

Así en diversos diarios españoles, académicos y abogados han resaltado el impacto de las seguridad de la información en los despacho de abogados.

"*Sin duda uno de los retos más importantes para los despachos es la ciberseguridad. Según explicaron los expertos en la materia, las firmas de abogados son objetivo de ataques porque manejan mucha información sensible y tradicionalmente no han tenido medidas de seguridad como las grandes empresas"*[16]

Así mismo lo señala Isabel Tovar [17] "*Dentro de un despacho de abogados se tratan diariamente datos sensibles*

que supone bienes intangibles de gran valor, tanto para los despachos como para sus clientes (...) La situación puede llegar a ser alarmante para el sector legal, ya que sus clientes ven amenazada la confianza que han depositado en estos profesionales ante la posible fuga de información u otras vulnerabilidades. Como consecuencia de esta problemática, los despachos de abogados deben llevar a cabo una estrategia de ciberseguridad para dar valor a sus clientes, evitando las filtraciones de información, repercusiones legales, sanciones y la posterior pérdida de imagen del despacho".

El Consejo General de Abogacía Española [18], ha diseñado una serie de decalogos y recomendaciones dirigidas a los profesionales del derechos, basado en el Reglamento General de la Protección de datos de la Unión Europea, que sin duda ha impactado a los despachos de abogados y las instituciones de Abogacía en España.

Fig 3. Decálogo de ciberseguridad de un despacho de abogados en España. [19]

El Consejo General de Abogacía Española recomienda se tengan en cuenta el anterior decálogo para efectos de contar con un despacho de abogados ciberseguro, así:

1. La creación de políticas y normativas o un Plan Director de Ciberseguridad que permita: identificar proceso críticos de la información, los empleados (abogados) y los equipos y activos que hacen parte del funcionamiento del despacho.

Fig 4. Decálogo de un despacho ciberseguro. Políticas y normativas. [20]

2. Establecer un control de acceso que permita definir qué usuarios pueden acceder al sistema de información del despacho de abogados.

Fig 5. Decálogo de un despacho ciberseguro. Control de accesos. [21]

3. Creación de copias de seguridad para proteger la información del despacho y garantizar la disponibilidad, integridad y confidencialidad de la misma.

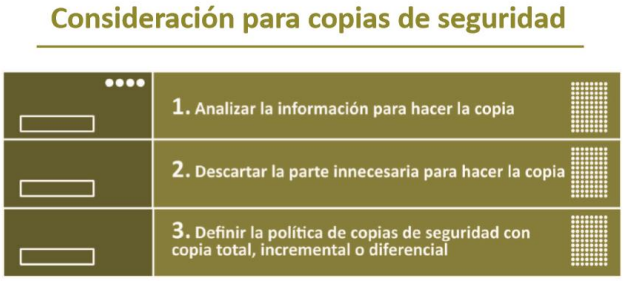


Fig 6. Decálogo de un despacho ciberseguro. Copia de seguridad. [22]

4. Desarrollar medidas necesarias para prevenir, detectar y contener cualquier tipo de amenaza de la información.

Fig 7. Decálogo de un despacho ciberseguro. Protección Antimalware. [23]

5. Efectuar un control sobre las actualizaciones de las aplicaciones que manejan la información.

Fig 8. Decálogo de un despacho ciberseguro. Actualizaciones. [24]

6. Asegurar el sistema de información de las amenazas provenientes de la web, el correo electrónico, mensajería instantánea y sistemas de almacenamiento online.

Fig 9. Decálogo de un despacho ciberseguro. Seguridad de la Red. [25]

7. Hacer un uso adecuado de herramientas como los dispositivos móviles y toda la información almacenada en dispositivos fuera del despacho de abogados. Aunque facilitan el acceso al trabajo, pueden ser un fácil acceso a la información.

Fig 10. Decálogo de un despacho ciberseguro. Información en tránsito. [26]

8. Contar con los medios y las técnicas que faciliten y permitan almacenar la información de la manera más adecuada.

Fig 11. Decálogo de un despacho ciberseguro.Gestión de Soportes. [27]

9. Monitorear con la finalidad de evaluar la calidad de los servicios prestados por el despacho de abogados

Fig 12. Decálogo de un despacho ciberseguro. Registro de actividad. [28]

10. Proteger los procesos principales del negocio con la implementación de estrategias que permitan a la organización recuperarse en caso de presentarse un incidente grave en un plazo de tiempo.

Fig 13. Decálogo de un despacho ciberseguro. Continuidad del negocio. [29]

VII. BENEFICIOS DE DESPACHOS DE ABOGADOS CIBERSEGUROS EN COLOMBIA

Como se ha venido mostrando, España ha sido un país líder en la construcción y aplicación de políticas y modelos para garantizar la seguridad de la información en el ejercicio de la labor de los abogados. Colombia ya cuenta con las herramientas necesarias para la construcción y aplicación de un sistema que permita proteger la información que manejan los

abogados en su quehacer diario. Sin embargo, esto no se hace y hasta ahora no sé le ha dado la importancia que debiera tener.

Para el desarrollo del presente artículo, se entrevistó a tres profesionales del derecho colombiano con experiencia en diferentes campos (notarial, litigioso y sector público), con el fin de mostrar, por un lado el desconocimiento frente a temas de ciberseguridad y protección de la información en el ejercicio de sus profesiones, así como la importancia y los beneficios de aplicar políticas de ciberseguridad como las expuestas en el capítulo VI del presente. De las entrevistas realizadas se pueden establecer las siguientes conclusiones [30]:

- Se tiene conocimiento de leyes relacionadas con la protección de datos personales. Sin embargo, se percibe que existe un conocimiento más profundo en el sector público, respecto del privado, en torno a la existencia de procesos relacionados con la seguridad de la información.
- La mayoría de la información que es administrada por los abogados en el ejercicio de su profesión es sensible y de su protección depende la seguridad de las organizaciones, de los clientes y del mismo abogado.
- En el Código Disciplinario del Abogado en Colombia se contempla el deber del secreto profesional. Con el desarrollo tecnológico actual y el uso de las tecnologías por parte de los abogados, es posible que el abogado incurra en una falta a este deber al no garantizar la protección de la información de sus clientes.
- El diseño de Despacho Ciberseguros en Colombia debe ir más allá de la protección de los datos personales. Deben implementarse igualmente políticas orientadas a la seguridad de la información y la aplicación de protocolos en casos como pérdida de información, ocasionada por fallas internas de la organización o por terceros. Lo anterior, como en el caso de España haciendo uso de políticas relacionadas como la continuidad del negocio.
- La tecnología también está presente en la labor de los abogados, por lo que es importante que estos conozcan como deben dar un uso responsable a la misma.

Los despachos de abogados colombianos deben optar por anticiparse a situaciones como fuga, robo o pérdida de información; haciendo uso como en el caso Español de políticas y normativas relacionadas con la protección y la seguridad de la información que manejan; creando controles de acceso a la información de sus clientes, copias de seguridad, protección ante virus o software maliciosos, dando un manejo adecuado de las actualizaciones de sus herramientas tecnológicas de trabajo, protección de la información almacenada con sus respectivos soportes, registro de las actividades y finalmente garantizar la continuidad del negocio frente a incidentes que puedan presentarse con la información que hace parte de sus procesos y sus clientes.

VIII. CONCLUSIONES

Muchos países alrededor del mundo han tenido que preocuparse por el manejo de los ciberataques y las amenazas provenientes del uso de la tecnología y los sistemas de información.

Los bufetes o despachos de abogados de la actualidad tienen el reto de adaptarse al uso de las nuevas tecnologías, no sólo disfrutando de sus bondades, sino teniendo un manejo responsable de los datos personales y sensibles de sus clientes y la información que hace parte de cada uno de los procesos judiciales que adelantan.

La protección de los datos personales, la confidencialidad, la integridad y la disponibilidad de la información deben ser elementos indispensables al interior de los despachos de abogados. La materialización de cualquier de las amenazas o riesgos por un inadecuado uso de la información puede ocasionar resultado indeseados en los procesos judiciales, graves perjuicios a los clientes y consecuencias para el despacho de abogados.

En países como España se ha profundizado en este tema, emitiendo recomendaciones y adoptando políticas y procedimientos dirigidos a la construcción y adecuación de despachos de abogados ciberseguros. Para esto ha acogido políticas similares a las que podemos encontrar en el Anexo A de la norma NTC-ISO-IEC 27001.

Colombia ha avanzado en la implementación de políticas y protocolos orientados a la seguridad de la información, especialmente en entidades del sector público y en las entidades financieras; por considerar que son éstas organizaciones más propensas a ser víctimas de ciberataques. Sin embargo, son los despachos de abogados organizaciones que administran un sin número de datos sensibles e información personal que deben proteger.

Es deber de todas las organizaciones, en este caso los despachos de abogados, buscar la forma de adaptar estas políticas al interior de sus procedimientos y garantizar el adecuado manejo de los datos personales y la seguridad de la información de los clientes que deciden confiar en ellos.

IX. REFERENCIAS

[1] Protección de datos y abogados: Conclusiones de la jornada del CGAE e INCEBE sobre Ciberseguridad. Disponible en:

https://www.abogadocompliance.com/proteccion-de-datos-y-abogados/
[2] Constitución Política de Colombia de 1991.
[3] Tipos de ataques Cibernéticos en Colombia. Disponible en: http://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf.
[4] Conpes 3701, Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación.
[5] Identificación de posibles acciones regulatorias a implementar en materia de Ciberseguridad. Coordinación Relaciones de Gobierno y Asesoría. Colombia. 2015. Disponible en: https://www.crcom.gov.co/recursos_user/Documentos_CRC_2015/Actividades_regulatorias/Ciberseguridad/Doc_Ciberseguridad28_07_15.pdf
[6] Conpes 3701, Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación
[7] Fiscalía General de la Nación. Boletín 23614. Fiscalía para Todos Radio. ¿Qué se debe tener en cuenta para ser un buen usuario de internet y no ser víctima de los ciberdelincuentes?
[8] Circular 007 de 2018. Superintendencia Financiera de Colombia
[9] Asobancaria. 2018. "La gestión de la ciberseguridad: un asunto de supervivencias para las organizaciones"
[10] Asobancaria. Sectores más atacados. Disponible en: http://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf
[11] Norma Técnica Colombiana NTC ISO/IEC 27001:2013
[12] Página Web Abogado Compliance. Disponible en: https://www.abogadocompliance.com/
[13] Código Disciplinario del Abogado. Ley 1123 de 2007. Colombia.
[14] Análisis del Deber de Secreto de la Ley Orgánica de Protección de datos en relación con el secreto profesional de los abogados. Beatriz Llorente Guillén. Universidad de Alcalá de Henares. España.
[15] La Ciberseguridad una amenaza real para los despachos: riesgos y retos. Disponible en: http://noticias.juridicas.com/legal-management-forum/inscribete/13208-la-ciberseguridad-una-amenaza-real-para-los-despachos-riesgos-y-retos/
[16] Siete retos en la gestión de despachos de abogados. Diario Expansión, Miércoles 26 de octubre de 2016. Disponible en: https://www.ontier.net/ia/retosgestiondespachosexpansion261016.pdf
[17] La innovación y la ciberseguridad revolucionan el negocio de los abogados. La transformación Legal y sus retos en el sector legal. Disponible en: https://www.ituser.es/whitepapers/content-download/7bdb3d6f-a7e0-4f42-9173-9f4509b601a2/especial-gmv-ituser035.pdf
[18] Órgano representativo, coordinador y ejecutivo de 83 Colegios de Abogados, a la cabeza de las profesiones jurídicas en España y Europa, creado desde Octubre de 1943.
[19] Decálogo de ciberseguridad de un despacho de abogados en España. https://www.abogacia.es/wp-content/uploads/2018/05/Decalogo-Ciberseguridad.pdf
[20] Ibidem
[21] Ibidem
[23] Ibidem
[24] Ibidem
[25] Ibidem
[26] Ibidem
[27] Ibidem
[28] Ibidem
[29] Ibidem
[30] Entrevistas realizadas a los abogados Liliana Ossa, Alejandra Tellez y Diego Hidalgo (Anexo 1)

ANEXO 1

Bogotá D.C. 16 de noviembre de 2018

ENTREVISTA 1

Las siguientes entrevistas se realizaron con el fin de mostrar la visión de algunos profesionales del derecho frente a la Ciberseguridad de la información en el ejercicio de su labor profesional.

Entrevistada: Lilia Patricia Ossa Colina: Coordinadora del área jurídica de la organización.

1. **¿En qué campo se desempeña y que experiencia tiene?**

Me desempeño como abogada asesora con el cargo de coordinadora jurídica en una notaria, y tengo una experiencia de 14 años.

2. **¿Conoce o sabe que avances ha hecho Colombia en cuanto a la seguridad de la información dentro de un bufete de abogados?**

La norma que aplicamos en la labor que hacemos en la notaria es la de protección de datos, Ley 1581 de 2012, que se maneja dentro del sector notarial.

3. **¿Qué tipo de información sensible maneja dentro de la oficina y cree que es importante protegerla?**

Sensible como lo determina la ley son orientación sexual, su religión, partido político, etc, lo que nosotros manejamos básicamente es su estado civil que es necesario para el trámite que se realicen en la notaria porque tienen unas implicaciones y es necesario saberlo, su identificación su dirección, número de teléfono entre otros.

Hay unos procesos en la notaría donde si puede a ver una información más sensible todavía, como es por ejemplo en el registro civil porque, es una información totalmente privada. En un registro civil de nacimiento hay información de quienes son sus padres, si la persona es adoptada, ese tipo de información que sólo le compete al que esté inscrito.

La experiencia mía es totalmente notarial, acá hay una tipo de información por ejemplo, un derecho de petición si hay ese tipo de cosas que pueden llegar aquí, y se refiere a una escritura pública, pues la escritura pública es eso, publica, entonces la información que está ahí la puede ver cualquier persona, en ese orden de ideas, digamos que el manejo de esa información y los datos que están ahí son de público conocimiento. No podríamos aplicarle en ningún momento reserva alguna porque la misma ley lo contempla así, porque son escrituras públicas, tendrían que hacer un reforma a toda la normatividad notarial para que exista la restricción en la información, porque de todos modos si no se tendría porque enterar de que "x" persona qué compro, cuánto le costó, cómo lo pago dónde vive etc, Esa información si puede resultar un poco compleja, que cualquier persona se entere de dónde vive, cuál es su número telefónico, cuál es su estado civil etc. Si valdría la pena que para ese tipo de información que además sólo le compete al que compra vende o hipoteca. Esa información no la debe tener todo mundo; sin embargo las escrituras están en disposición del que venga a revisarlas.

Total, esa información la pueden utilizar para evidentemente extorsionar a cualquier persona, para hacerle seguimiento a una persona. Yo pienso que todo lo que uno haga debe ser privado y quedarse en eso en privado. No hay razón para que uno quede expuesto públicamente con algo que es mío, sólo a mi me importa. Es importante sobre todo en la labor que hacemos notarial que si debería a ver una restricción total también para las escrituras.

4. **¿Qué riesgos de la seguridad de la información considera que hay en la labor del abogado?**

A nivel general el abogado viene siendo un confesor, la misma normatividad que tiene el abogado como tal lo obliga a tener reserva de lo que sabe de sus clientes, lo digo a nivel general, el también tiene el derecho a guardar ese secreto profesional como lo hacen los médicos. en ese sentido. Ahora si el abogado que viola

su ética y difunde una información que le fue conferida, la ley puede amparar a la persona que se sienta afectada

5. **¿Conoce algún caso real en donde se haya vulnerado la información sensible de algún cliente y de qué forma lo ha perjudicado?**

No, información sensible como tal no, digamos que en este mundo notarial se ve, es que de pronto suplantan alguna persona y hacen negocios fraudulentos, ese tipo de cosas. Lo que hablábamos con anterioridad porque una persona puede pedir una copia de una escritura, tiene toda la información y me pueden cambiar la escritura y pueden suplantarme, en ese orden de ideas, demandas hay muchas.

6. **¿Qué impacto tendrá para su oficina si un tercero se infiltrará y robara la información de los usuarios?**

En este campo notarial la información ni siquiera la tienen que robar, solo con el simple hecho de que vengan a pedir una copia de una escritura y ahí quedan legalmente informados de lo que necesiten, ahora el tema es si me dejan a mi sin información sería grave porque si se roban un tomo pero tengo digitalizada la escritura, la ley me permite reconstruir esas escrituras pero si no lo tuviera?

Si se robaran toda la información imagínate todas las demandas, y si por causa de ese robo Ha perjudicado a un comprador, las demandas a la notaria serian grandísimas.

7. **¿implementaría algún sistema de seguridad de la información dentro su despacho de abogados?**

Para efectos de temas notariales, pienso que se debería cambiar el estatuto y como toda la concepción del tema notarial, y dejarlo privado, es una Información privada y sólo debería pedir copias el interesado, un juez o para alguna investigación, y si viene algún tercero que sea con autorización del interesado, a nadie más le puede interesar una escritura pública de compraventa.

La anterior encuesta cuenta con la autorización de la Doctora Lilia Patricia Ossa Colina Coordinadora del área jurídica de la organización, para que se muestre su nombre y sus respuestas para fortalecer la realización del artículo “La Ciberseguridad en el Ejercicio de la Abogacía”.

Bogotá D.C. 16 de noviembre de 2018

ENTREVISTA 2

Entrevistada: María Alejandra Téllez Méndez: Abogada litigante experta Derecho Laboral y Seguridad Social

1. **¿En qué campo se desempeña y que experiencia tiene?**

Yo me desempeño en el campo de Derecho Laboral y Seguridad Social. Soy abogada litigante hace más o menos 7 años en Bogotá.

2. **¿Conoce o sabe que avances ha hecho Colombia en cuanto a la seguridad de la información dentro de un bufete de abogados?**

No conozco específicamente, pero digamos que cada vez se ha avanzado más en sistematizar la información entonces, anteriormente, para consultar un proceso en los juzgados se debía ir directamente hasta el Juzgado y cada Juzgado manejaba un computador donde se hacía la alimentación de la actualizaciones o las anotaciones de cada proceso. Eso hacía que la labor de seguimiento de los procesos fuera más dispendioso, más lenta porque no había un sistema unificado, había que ir juzgado por juzgado consultando los procesos. Muchos de ellos no tenían computadores, entonces sólo manejaban estado impresos, eso no hacía fácil la gestión para los bufetes de abogados porque tenían que estar todo el tiempo en constante seguimiento de los procesos por medios físicos directamente. Mas o menos en el año 2010 se empezó a implementar el sistema de información unificado para la rama judicial y ya digamos que a través de internet se podía consultar los procesos de cualquier ciudad de país siempre y cuando estuviera dentro de ese sistema y podía obtenerse la información en tiempo real.

En la empresa en la que yo trabajo a raíz de esa sistematización que hubo en el sistema de la rama judicial se diseño un sistema de información para los clientes donde no solamente se tiene la información en tiempo real del expediente como tal, de la actuación judicial o administrativa que se realice sino que también el cliente puede obtener información de los documentos de su proceso de forma segura porque se les crea una clave y un usuario para ingresar de tal forma que se garantiza que solamente su abogado y el cliente directamente puedan tener acceso a la información haciendo el seguimiento respectivo con la clave y el usuario que se le da desde el inicio de la gestión. Entonces la sistematización de la rama judicial le permitió por lo menos a nuestra empresa, diseñar un programa donde pudiéramos tener la información en tiempo real pero además de forma segura y actualizada.

No conozco mucho de sistemas, no se si puedan hackear por ejemplo el sistema de información de nuestra empresa, eso no lo sé. Lo que si sé es que por ejemplo para ingresar a ese sistema tu debes tener una clave y un usuario y esa clave y usuario únicamente lo pueden manejar funcionarios de la empresa que tienen acceso a la información o los clientes de la empresa. Si el cliente comparte su clave, su usuario, obviamente estaría en riesgo la información pero sería porque él mismo lo permito. O si algún trabajador deja de pertenecer a la compañía, esa clave y usuario se inactiva. Por ese lado digamos que estaría blindada la información. Pero de sistema de seguridad no sé, entonces no sé si de pronto tengamos algún antivirus o algo que nos proteja por ejemplo de un Hacker que quiera entrar a nuestra información, porque en ultimas está en la nube. Entonces si alguien Hackea el sistema podría ingresar de pronto a nuestro sistema y descargar documentos sensibles como Resoluciones, copias de cédula, certificaciones.

3. **¿Qué tipo de información sensible maneja dentro de la oficina y cree que es importante protegerla?**

Nosotros manejamos documentos como: la copia de la cédula de ciudadanía, que es sensible porque sirve para hacer muchísimas cosas, declaraciones de renta, información sobre ingresos de la persona, certificados laborales, registros civiles de sus hijos. Nosotros en general toda la información que manejamos es información sensible. Si eso llegará a ser conocido por terceras personas con otras intenciones podrían ser utilizadas o en otros procesos o para hacer algún tipo de requerimiento, por ejemplo, un embargo, una presunción de ingresos. Si es información sensible la que nosotros manejamos y por eso en el contrato que nosotros firmamos con el cliente hacemos un pacto de confidencialidad de la información y de los documentos.

Es importante protegerla, porque yo pienso que si el cliente está brindándonos esa información y esos documentos que pueden ser utilizados por terceras personas con otras intenciones, será deber del abogado guardar la reserva de esos documentos y por eso la Ley de protección de datos aplicaría acá, porque nosotros como abogados así no seamos empresa, inclusive el abogado litigante que es independiente debe tener una autorización por parte de su cliente expresa y firmada donde el cliente autoriza utilizar esa información y para qué fines. No necesariamente puede hacer una autorización abierta, sino debe ser una autorización limitada a los fines por ejemplo del poder o del contrato de prestación de servicios profesionales que hayan firmado, porque esa información al ser tan sensible y más en este ámbito jurídico, si se puede utilizar para otras cosas.

4. **¿Qué riesgos de la seguridad de la información considera que hay en la labor del abogado?**

Considero que hay una estrecha relación entre el deber de proteger los datos por parte del abogado y el secreto profesional. Nosotros si tenemos esa responsabilidad frente al cliente así no haya una manifestación expresa que diga que esos documentos se los deba guardar con reserva. Si el cliente me confía a mi toda la información de sus finanzas.

5. **¿Conoce algún caso real en donde se haya vulnerado la información sensible de algún cliente y de qué forma lo ha perjudicado?**

No, no tengo conocimiento de un caso así.

6. **¿Qué impacto tendrá para su oficina si un tercero se infiltrará y robara la información de los usuarios?**

Eso sí sería grave porque el cliente no volvería a confiar en nosotros y eso si podría generar perjuicios tanto como empresa, como profesionales en derecho porque el cliente no solamente podría denunciar a la empresa, sino podría denunciar al abogado como sujeto disciplinable, precisamente por no proteger la información que dio con reserva ese cliente. Y si puede demostrar que le causó unos perjuicios con mayor razón.

Nosotros principalmente tuvimos un incidente porque entró un correo con virus al sistema y eso hizo que nos bloquearan las cuentas empresariales y tuvo un gran impacto en el servicio al cliente porque no solamente se perdieron algunos correos electrónicos o no llegó la información a los clientes eso también genera inseguridad para el cliente, porque asume que nosotros tenemos previsto ese tipo de riesgos o de situaciones, como por ejemplo eso, un correo con virus. Se supone que la empresa debería tener una estrategia de cómo actuar en ese tipo de situaciones, unos correos de respaldo por ejemplo, pero la empresa sólo hasta cuando sucedió el incidente se dio cuenta que proveedor no respondía a las necesidades de la empresa, pero sólo hasta cuando sucedió eso. Entonces si afecta, porque no sólo se pierde la información, se pierde la confianza con el cliente y en algún caso extremo se podría perder la información que tenemos en la nube subida referente al sistema de información que tenemos. Si se pierde el contacto con el cliente se pierde toda la confianza y se pueden perder los clientes, eso sería un impacto gravísimo. Sólo hasta que es nos sucedió nos dimos cuenta que si es relevante para la empresa el manejo de la información y todos esos mapas de riesgos que deben tener previstos la empresa para saber cómo actuar o con qué protocolo enfrentar una situación así.

7. **¿Implementaría algún sistema de seguridad de la información dentro su despacho de abogados?**

Yo considero que siempre debe haber un líder del proceso, una sola persona que cree, elimine y modifique claves y contraseñas. Lo que permitiría que ese fuera el enlace de seguridad siempre. Pues si hay más de una persona con acceso a esa información y permisos, hay mayor riesgo de que otras personas manipulen la información. Considero que deben diseñarse planes de choque frente a situaciones como la que he descrito.

La anterior encuesta cuenta con la autorización de la Doctora Alejandra Tellez, Abogada Litigante experta en Derecho Laboral y Seguridad Social, para que se muestre su nombre y sus respuestas para fortalecer la realización del artículo “La Ciberseguridad en el Ejercicio de la Abogacía”.

Bogotá D.C. 17 de Noviembre de 2018

ENTREVISTA # 3

Entrevistado: Diego Fernando Hidalgo Umbarila: Abogado funcionario del sector defensa.

1. **¿En qué campo se desempeña y que experiencia tiene?**

Me desempeño en el área de seguridad documental específicamente en el campo jurídico de la documentologia, dactiloscopia y grafología y tengo 4 años de experiencia.

2. **¿Conoce o sabe que avances ha hecho Colombia en cuanto a la seguridad de la información dentro de un bufete de abogados?**

Colombia a través de sus entidades públicas ha realizado avances en cuanto a la seguridad de la información en cuanto a que ha implementado tanto en las oficinas jurídicas como en general el cumplimiento y certificación de la norma iso 27001 de icontec (relacionada con la seguridad de información) estando a la vanguardia de estándares internacionales.

3. **¿Qué tipo de información sensible maneja dentro de la oficina y cree que esta es importante protegerla?**

En el desempeño de mi labor manejo información pública privada y confidencial relacionada con las fuerzas militares y es importante protegerla para el equilibrio social económico del país.

4. **¿Qué riesgos de la seguridad de la información considera que hay en la labor del abogado?**

En la labor de abogado existen riesgos de la seguridad de la información tales como la fuga de información por parte del algún Integrante de la oficina, ataques informáticos, infiltración de personal no autorizado entre otros.

5. **¿Conoce algún caso real en donde se haya vulnerado la información sensible de algún cliente y de qué forma lo ha perjudicado?**

Si conozco un caso real donde se vulneró información confidencial de personal de la fuerza pública como datos biográficos y de ubicación. Con esto se ocasionó un gran perjuicio pues el desenlace fue que perdió la vida.

6. **¿Qué impacto tendrá para su oficina si un tercero se infiltrará y robara la información de los usuarios?**

El impacto ante el robo de información implicaría un daño directo a los usuarios al sector defensa y colateral a los familiares y la sociedad en general ya que podría ocasionar un desequilibrio social.

7. **¿Implementaría algún sistema de seguridad de la información dentro su despacho de abogados?**

Si claro implementaría el cumplimiento estricto de la norma ISO 27001 de icontec y sería objeto de auditoría cada año para renovarla así como la última tecnología en seguridad informática.

La anterior encuesta cuenta con la autorización de la Diego Fernando Hidalgo Umbarila funcionario del sector defensa para que se muestre su nombre y sus respuestas para fortalecer la realización del artículo “La Ciberseguridad en el Ejercicio de la Abogacía”.